

REMARKS

These remarks are set forth in response to the non-final office action mailed October 20, 2005 (the "Office Action"). As this amendment has been timely filed within the three-month shortened statutory period, neither a petition for an extension of time nor a petition fee is required. Presently, claims 1 through 20 are pending in the Patent Application. In the Office Action, each of claims 1 through 20 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,724,578 to Morinaga et al. (Morinaga) in view of U.S. Patent Application Publication No. 2002/0035697 to McCurdy et al (McCurdy) and further in view of U.S. Patent Application Publication No. 2002/0178271 to Graham et al. (Graham).

In response, the Applicants respectfully traverse the rejections on the art and request that the Examiner reconsider the suitability of Graham as a reference as the Applicants' careful reading of paragraphs [0140] and [0141] reveal that while a "filter-driver" can be used to "intercept and modify" a file system request, no where in paragraphs [0140] and [0141] is it stated or suggested that the "filter-driver" can "suppress" a file system request as required by the language of the Applicants' independent claims. Prior to addressing the rejections on the art, however, a brief review of the Applicants' invention would be appropriate.

The Applicants have invented a new, useful and non-obvious system and method for managing both access to and digital rights in secure files in a collaborative environment. Generally, a collaborative environment can include one or more persons sharing files across one or more computing devices such as personal computers, handheld computers, personal digital assistants and the like. When configured for use with a particular authoring application, files created using the authoring application can be securely shared with other collaborators using the

same authoring application. In particular, access to an authored file can be limited according to the preferences of the file author. These limitations can include not only absolute limitations, for instance the identity of a collaborator who is permitted to access and whether collaborators can save, modify or print the file, but also intermediate limitations, for example periods of time during which collaborators can access the file.

In a preferred aspect of the present invention, collaborative files can be secured through a combination of encryption, access policy specification and digital rights management. In particular, once encrypted, the file can be associated with a digital container which specifies both the access policy pertaining to the file and digital rights managing the level of access permitted in the file. The access policy can identify the type of user or users who are permitted to access the file. The access policy also can specify a time period during which users can access the file. Still, the access policy is not limited to the examples specified herein and the access policy can include any time of access limitation which generally limits access to the file based upon the identity of the user, the contents of the file or the period when the file can or cannot be accessed.

The digital rights, by comparison, can specify those operations which can be performed on the file once a user has been granted access to the file. Digital rights can include any type of operational limitation, for example whether a user can print, save, copy, or modify the file. Notably, the digital rights can vary according to the identity or class of user, however, in a preferred aspect of the invention, digital rights can be specified by the author, or by default, independently from the access policy.

Importantly, files which have been secured in accordance with the inventive arrangements can be distributed without requiring collaborators to maintain network access to a

centralized server in which access to the distributed files can be managed. Rather, access to secured files can be managed locally, from within the computing device in which a collaborator attempts to access the secured file. In this regard, access to each secured file can be managed according to the access policy and digital rights specified in the digital container appended to the secured file. Also, unlike prior art digital rights management systems, collaborators can access secured files transparently and seamlessly through the authoring application without requiring the collaborator to invoke third party security applications. *Significantly, the seamless and transparent access to secured files through an authoring application can be facilitated through the trapping and suppression of file I/O requests issued by the authoring application.*

More specifically, exemplary independent claim 1 and 13 recite a methodology and apparatus having the following steps:

- (A) identifying a file input/output (I/O) request to access a file, said file I/O request originating in an authoring application;
- (B) suppressing said file I/O request;
- (C) automatically extracting digital rights management data appended to said file;
- (D) providing said file to said authoring application; and,
- (E) managing access to said file in said authoring application based upon said extracted digital rights management data.

Steps A through C relate to the interception of a file I/O request originating from an authoring application. Steps D and E relate to the use of digital rights management data retrieved from a file associated with the file I/O request in the course of managing access to the file in the authoring application. Thus, as it will be apparent from the plain language of claims 1

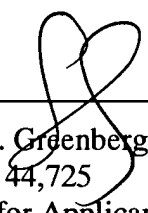
and 13 (and also independent claims 9 and 12), **suppressing file I/O requests** in respect to the seamless management of digital rights in an authoring application is central to the Applicants' invention.

Importantly, the cited portion of Graham wholly lacks any reference to the **suppression** of file I/O requests as explicitly recited in all of the independent claims. Rather, Graham only teaches the interception and modification of file requests. In particular, the first sentence of paragraph [0141] of Graham is telling, "This filter driver allows the client module 230 to intercept and modify file requests to and from file servers as required." Accordingly, it will be clear from this statement that file requests are not "suppressed" as required by the language of the Applicants claims 1, 9, 12 and 13, but merely modified.

In view of the foregoing remarks, the Applicants respectfully request the withdrawal of the rejections on the art based upon the Morinaga, McCurdy and Graham references. The Examiner is encouraged to telephone the undersigned to discuss any matter that would expedite allowance of the present application.

Respectfully submitted,

Date: January 20, 2006



---

Steven M. Greenberg  
Reg. No.: 44,725  
Attorney for Applicant(s)  
Christopher & Weisberg, P.A.  
200 East Las Olas Boulevard, Suite 2040  
Fort Lauderdale, Florida 33301  
Customer No. 31292  
Tel: (954) 828-1488  
Fax: (954) 828-9122